IEEE P802.11

Wireless Access Method and Physical Layer Specification

Addition of a Key ID Field

Michael Fischer
Digital Ocean, Inc.
4242–3 Medical Drive
San Antonio, TX 78229
Telephone: +1–210–614–4096
Facsimile: +1–210–614–8192
email: mfischer@CHILD.com

Summary

This submission contains modifications to the contents of sections 5.2 and 5.3 to add a key ID subfield to the IV field of WEP frames This mechanism is important to support many key management mechanisms which otherwise could not be used in for WEP key management. See document 95-187 for discussion of the reasons for this recommendation. Voters favoring this proposal can cite this document as the source of replacement text for their D2.0 letter ballot comments.

NOTE TO EDITORS: These text changes should be applied AFTER the editorial corrections to sections 5.2 and 5.3 contained in document 95–212 (which were adopted at the July, 1995 meeting but not fully applied to the D2.0 text).

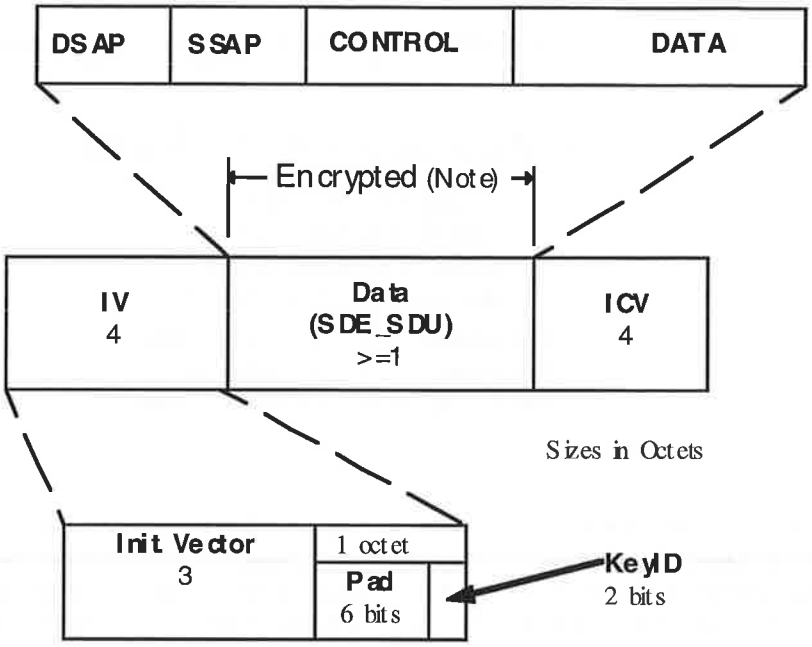
Changes to Section 5.2.5

Figure 5-4 shows the encrypted MSDU as constructed by the WEP.

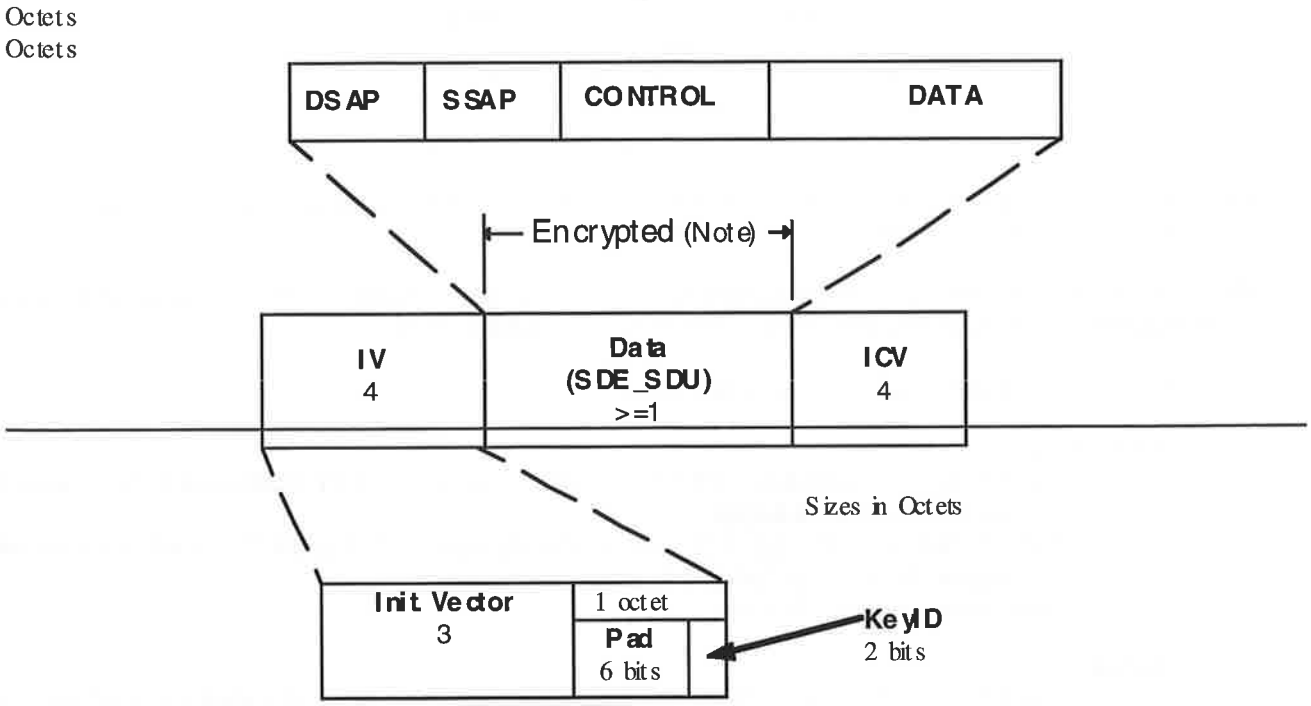
The WEP ICV = 32 bits. The expanded MSDU shall include a 32 bit IV field immediately preceding the MSDU. This field shall contain three~~two~~ sub-fields: A 3-octet field that contains the initialization vector, a 2–bit KeyID field, and a 6–bit ~~1–octet~~ pad field to maintain even–octet alignment of the encrypted payload. The KeyID field contents select one of four possible secret key values for use decrypting this MSDU. Interpretation of these bits is discussed further in section 5.3.2. The contents of the pad field shall be zero. The KeyID occupies the two least significant bits of the last octet of the IV field, while the pad occupies the six most significant bits of this octet.

The WEP mechanism is invisible to entities outside the 802.11 MAC.

Octets
Octets



Note: The encipherment process has expanded the original MSDU by 8 Octets, 4 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only.



Note: The encipherment process has expanded the original MSDU by 8 Octets, 4 for the Initialization Vector (IV) field and 4 for the Integrity Check Value (ICV). The ICV is calculated on the Data field only.

Figure 5-4: Construction of expanded WEP MSDU

Changes to Section 5.3.2

The default value for all WEP keys shall be Null. This indicates an invalid WEP key. An attempt to use WEP with a Null key shall result in an error condition.

To support shared key configurations, the MIB contains a 4-element vector ~~variable~~ called "aDefault_WEP_Key". The default value for each element of this vector~~this variable~~ is Null. If not null, these elements~~is variable~~ contains the deafault keys to be used with WEP. For transmitted MSDUs the value of aWEP_Default is used to select the element from this vector from which to obtain the encryption key, as well as the value to transmit in the KeyID field. For received MSDUs the value from the KeyID field is use to select the element from this vector from which to obtain the decryption key.

An additional variable called "aWEP_Default" is an integer ~~boolean~~. If set to a value of 0, 1, 2, or 3 ~~True~~ then on transmit, Data frames shall be encypted using the corresponding element from aDefault_WEP_Key and on receive they shall be decrypted using the element from aDefault_WEP_Key selected by the received KeyID field. When aWEP_Default set to any other value, the contents of aWEP_Default are not used for WEP. The MIB shall not allow aWEP_DEfault to be set to values 0, 1, 2, or 3 ~~TRUE~~ if the corresponding element of aDefault_WEP_Key is Null. The default value of WEP_Default is 4 ~~False~~. The value in the transmitted KeyID field is zero in all cases except when set to a value of 1, 2, or 3 due to the transmission behavior discussed above.

802.11 does not require that the same WEP key be used for all stations. The MIB supprts the ability to have a separate WEP key for each station which which a Station directly communicates. This is supported by a MIB variable which is a two dimensional array called "aWEP_Key_Mapping". The array is indexed by MAC address and contains two fields for

each entry: "WEP_ON" and the corresponding WEP_Key. The MIB shall not allow WEP_ON to be set to TRUE if the corresponding WEP_key entry is Null. The default value for all WEP_ON fields is False. This variable is always indexed by either RA to TA addresses (since WEP is applied only to the wireless link).

The values in this array variable take precedence over the aWEP_Default and aDefault_WEP_Key variables.

The minimal length of aWEP_Key_Mapping shall be 10. This value represents a minimum capability that may be assumed for any station which implements the WEP option.

The maximum length of aWEP_Key_Mapping shall be implmementation dependant and the actual length of the array can be inquired from the read only MIB variable "aWEP_Key_Mapping_Length".

The interactions between these variables is described below:

Transmit case:
if aWEP_Key_Mapping(RA, WEP_On) = Trure then use aWEP_KEY_Mapping(RA, WEP_Key) for encryption, transmit KeyID =0,
if aWEP_Default = { 0 | 1 | 2 | 3 } ~~Ture~~ then u~~U~~se aDefault_WEP_Key(aWEP_Default) for encryption, transmit KeyID =aDefault_WEP_Key,
otherwise do no encypt the frame.

Receive case:
if aWEP_Key_Mapping(TA, WEP_On) = Trure then use aWEP_KEY_Mapping(TA, WEP_Key) for decryption,
if aWEP_Default = { 0 | 1 | 2 | 3 } ~~Ture~~ then u~~U~~se aDefault_WEP_Key(received KeyID) ~~Default~~ for decryption,
otherwise do no attempt to decypt the frame.

MIB Definitions to change in appropriate subsection of Section 8.4

aWEP_Default

```
WEP_Default ATTRIBUTE
WITH APPROPRIATE SYNTAX
    Integer;
BEHAVIOUR DEFINED AS
    "This attribute shall indicate that use of the corresponding element of the Default_WEP_Key array when set to
    values of zero, one, two, or three; or that the Default_WEP_Key values are not to be used when set to any other
    value.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(10036) SMT(0) attribute(7) wep_default(#) };
```

aDefault_WEP_Key

```
Default_WEP_Key ATTRIBUTE
WITH APPROPRIATE SYNTAX
    << however you declare a 4–element array of 40–bit integers in ASN.1 >>;
BEHAVIOUR DEFINED AS
    "This attribute shall contain the four default WEP secret key values corresponding to the four possible KeyID
    values.";
REGISTERED AS
    { iso(1) member-body(2) us(840) ieee802dot11(10036) SMT(0) attribute(7) default_wep_key(#) };
```